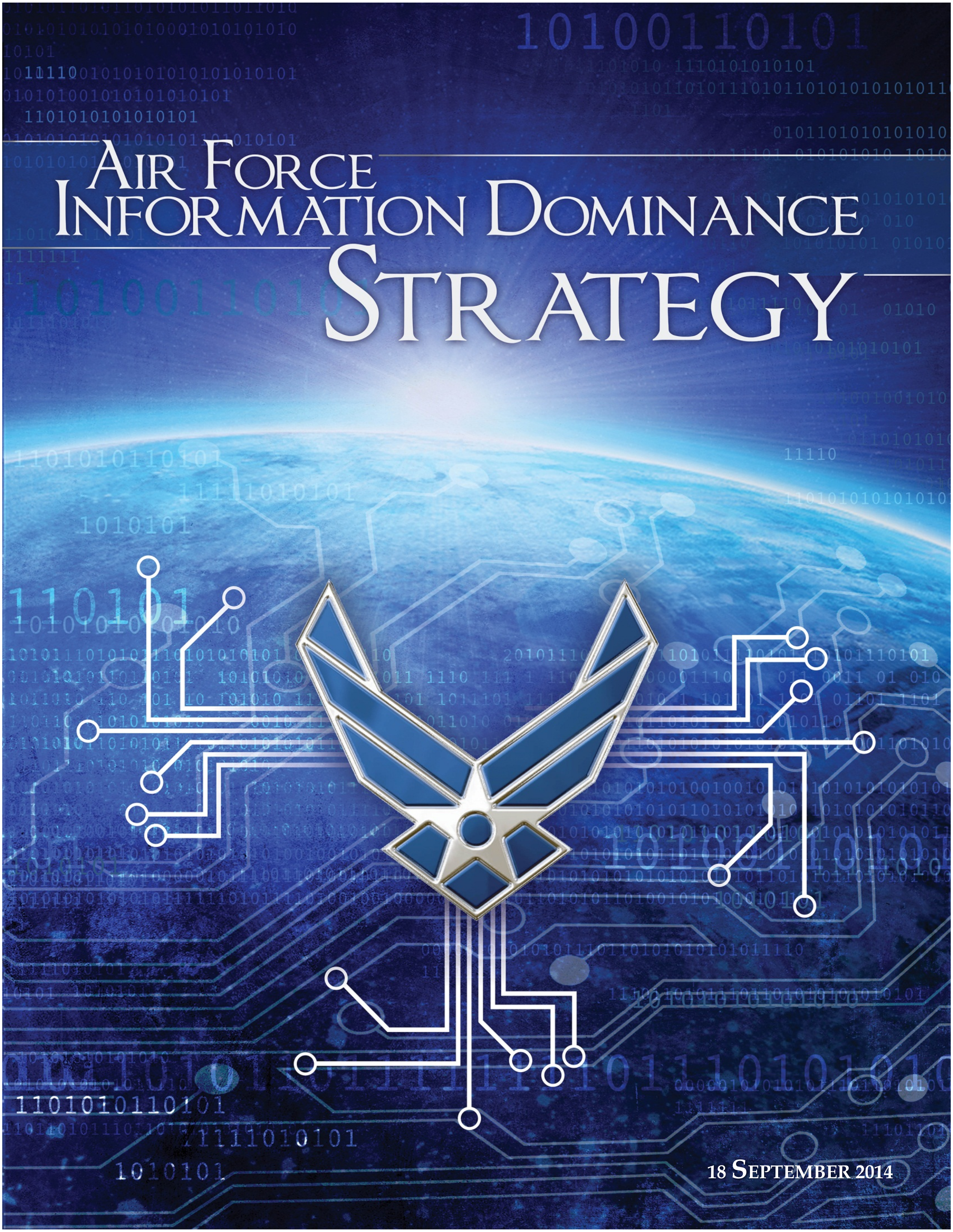
Air Force Information Dominance Strategy



18 September 2014

FOREWORD

Since the Air Force's founding, Airmen have led in development, integration, fielding and sustainment of cutting-edge weapon systems vital to the security of America and its allies. The ability of the Air Force to imagine and deliver superior, cyberspace-secure weapon systems strengthens our Nation. This strength stems in large measure from the ingenuity of our Cyber-Airmen workforce, uniting with the rest of the operational community, industry, and academia to deliver game-changing technological advancements, information systems, and systems-of-systems and making trusted information available where and when needed.

This Information Dominance Strategy for the United States Air Force projects forward 10 years. It is designed to address the demands of the strategic environment faced by the entire Air Force – active, guard, reserves, and civilians. It provides a strategic framework that encompasses the cyberspace domain. It articulates challenges faced by the Air Force and provides for unity of purpose and effort in overcoming those challenges with coherent action to realize the Information Dominance Vision: The Air Force fully exploits the man-made domain of cyberspace to execute, enhance and support Air Force core missions.

This strategy aligns with the strategies of the Air Force and the Department of Defense (DoD). It moves the focus of the cyberspace community from one of providing "core services" and executing cyberspace operations to instead focus on Cyber-Airmen executing, enhancing, and supporting Air Force core missions. That distinction is important. For it is to Air Force core missions that all of our efforts will ultimately contribute.

This strategy is designed to provide direction for mission area roadmaps that guide the future Enterprise Architecture and provide the systematic alignment of effort and resources across all Air Force components. It will be revisited every two years to ensure relevance and coherence to Air Force, DoD, and national strategic objectives. Comments regarding it can be directed to my Strategy and Policy Division - usaf.pentagon.saf-cio-a6.mbx.a3cs-a6cs-strategy-and-policy@mail.mil

MICHAEL J. BASLA, Lt Gen, USAF
Chief, Office of Information Dominance and
Chief Information Officer

EXECUTIVE SUMMARY

This document provides a framework for coordinating movements by multiple organizations and thousands of individuals working to provide **information dominance**[1] for the United States Air Force. This is challenging. Why? In part because the domain in which we operate in and through (cyberspace) is also created and affected by our decisions about what to build and by the decisions of every Airman who will log in and use or provide data. It is also challenging because the enemy gets an asymmetric vote on how, when, and whether to exploit any vulnerability we may not know about, have overlooked as insignificant, or have left unguarded.

The vision is for the Air Force to fully exploit the man-made domain of cyberspace to execute, enhance and support Air Force core missions. Our strategic aim is to push and pull trusted information to and from Airmen as effectively as possible so they can make informed decisions to execute their mission. This simple aim implies much work ahead. To meet this aim, we start by defining three tenets for Information Dominance:

1. Increase effectiveness of Air Force core missions.
2. Increase cybersecurity of Air Force information and systems.
3. Realize efficiencies through innovative IT solutions.

Our Airmen need trusted information in garrison and across the range of military operations to conduct their missions. There is a need for fewer systems and simpler human and machine interfaces. Our systems need to be resilient and trustworthy and the Cyber-Airmen who provision, operate, maintain, and use the systems need expertise both in exploiting cyberspace and the core missions to which they contribute. Four goals articulated in this document will move the Air Force to overcome the challenges posed by systems-of-systems complexity and cyberspace vulnerabilities:

1. Provide Airmen trusted information where they need it so they can be most effective.
2. Organize, train and educate Cyber-Airmen to be experts in cyberspace and the Air Force core missions to which they contribute.
3. Strengthen mission assurance through freedom of maneuver in and through cyberspace.
4. Optimize the planning, programming and execution of cyberspace investments.

Goals describe the ends, but are insufficient to describe needed action; therefore this document also articulates objectives that provide specific, measureable actions that will realistically move the Air Force toward achieving each goal. The deliberate decision to focus our efforts and resources toward these goals means we will focus on the highest priority items and cease efforts

[1] Information Dominance definition: “The operational advantage gained from the ability to collect, control, exploit, and defend information to optimize decision making and maximize warfighting effects.”

and investments on activities that are tangential or unrelated. With thousands of individuals and hundreds of organizations across core functions, there will be many coordinated steps that need to be taken to achieve these Air Force objectives. The Mission Area Roadmaps will provide further, detailed direction and the corporate portfolio management processes will appropriately align Air Force resources toward these ends.

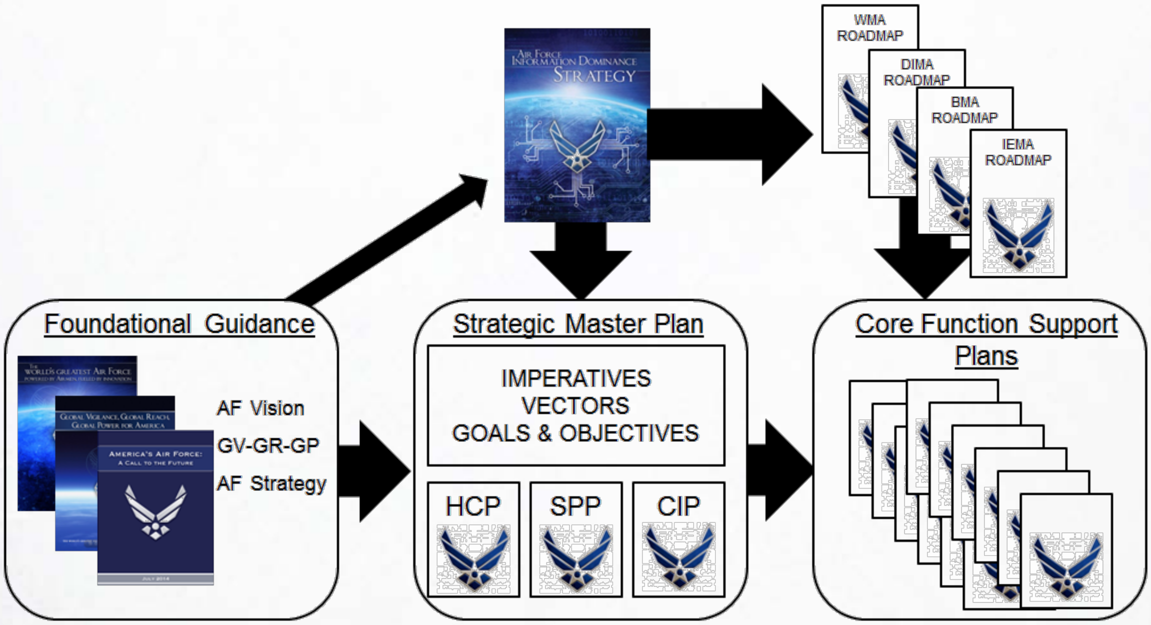


Figure 1. AF Information Dominance Strategy Relationship to the new Air Force Strategic Planning Process (AFPD 90-11, *Strategic Planning System*)

TABLE OF CONTENTS

STRATEGIC ENVIRONMENT AND CHALLENGES

The United States Air Force's mission is to *fly, fight and win… in air, space and cyberspace.* This mission requires exceptionally well-trained Airman and sophisticated equipment around the world. The Air Force protects and preserves our Nation's security interests, and offers freedom of action to our Joint and Coalition partners, by integrating missions to provide Global Vigilance, Global Reach, and Global Power.[2] This is the Air Force Vision, [3] achieved through unmatched execution of five core missions: air and space superiority; intelligence, surveillance, and reconnaissance (ISR); rapid global mobility; global strike; and command and control (C2).

Cyberspace is an operational domain. Our ability to operate in and through the cyberspace domain benefits every core mission through increased and improved speed, ubiquity, access, stealth, surprise, real-time battlespace awareness and information exchange, and command and control. Virtually every mission across the range of military operations depends on the robust and resilient availability of a secure and trusted cyberspace domain. Every capability, mission, and member of the Air Force depends on Information Dominance for success. Although most of the cyberspace domain is not under military or even U.S. Government control, the DoD operates within this global domain and defends those operations, systems and information.

Risks exist in every domain, but because of the globally interconnected nature of cyberspace, and the operational need for Air Force systems to "trust" each other, a cyberspace vulnerability in any one system introduces potential risk to all systems and, by extension, the users of and information on those systems. This is the "physics" of cyberspace. However, unlike risks inherent in the physics of other operational domains, we can mitigate vulnerabilities and manage risk in cyberspace through manipulation of the domain itself.

The Air Force's technological advantage is challenged by the worldwide proliferation of advanced technologies, including integrated air defenses, long-range ballistic and cruise missiles with precision-capable warheads, and advanced air combat capabilities. Advances in adversarial capabilities in space control and cyber warfare may also challenge U.S. freedom of action. Some of these capabilities are attained with relatively minimal cost, greatly reducing the barriers to entry that have historically limited the reach and power of non-state actors, organized militias, and radical extremists.

We live in an age of surprise, where individual acts can be powerful and the effects can be global. Today's strategic environment presents a broad range of threats and an unpredictable set of challenges, ranging from non-state actors to nuclear armed nations. This requires flexibility, versatility, and a shift to inherently agile, deployable, and networked systems from those designed for fixed purposes or limited missions.[4]

[2] AF Global Vigilance, Global Reach, Global Power for America, 2013.

[3] US Air Force Vision, 2013.

[4] USAF Posture Statement, 2014.

The future is challenging to predict in the technology arena. Rapid advances exploited by growing and increasingly sophisticated international competitors have created an environment today in which operational and strategic risks introduced by cyberspace vulnerabilities are both diffuse and potentially catastrophic. Our contemporary cyberspace forces are faced with a proliferating array of mission systems with ever more mutual dependencies and unexpected cyberspace vulnerabilities. This reflects the Air Force's past approach of delivering individually exquisite systems rather than delivering integrated warfighting capabilities.

Defense of the Air Force Information Network is conducted through Air Force cyberspace operations, specifically by Cyber-Airmen conducting Department of Defense Information Network Operations (DoDIN Ops) and Defensive Cyberspace Operations (DCO) in coordination with other services and agencies of the government. However, the relative advantage in expertise enjoyed by the United States (and the Air Force's ability to recruit top talent) is under pressure as rising percentages of college degrees in science, technology, engineering, and mathematics are awarded to citizens of competitor-nations, even by American universities.[5]

Emerging global trends provide further insight and set a context to inform cyberspace directions. Some of these emerging trends in technology indicate a closer human-machine interface that includes cloud computing, smart machines, continued proliferation of mobile devices, the "Internet of Things," and software-defined everything.[6] Winning wars improves with the ability to adapt to a changing environment to gain and maintain information dominance despite emerging, highly adaptable and asymmetric adversaries and threats (whether they are nation states or non-state actors).

For mission success in tomorrow's congested and contested information environment, the Air Force requires centralized strategic direction in developing and assuring operations in and through cyberspace. Unity of efforts and optimized investments will better afford seamless interoperability, resilience,[7] and flexibility that will be both responsive to technological change and sustainable in the resource-constrained environment of the next decade.

Some of the specific challenges we foresee for the Air Force in building, extending, and securing the Air Force cyberspace domain toward 2023 include the following:

1. Solving communications and computing constraints related to Tactical Edge environments (disconnected or intermittent connectivity, limited throughput, high latency and jitter, and low-power).

2. Ensuring the electromagnetic spectrum is available for future military usage in the face

[5] *Department of Commerce 2012 report on competitiveness*, http://www.commerce.gov/sites/default/files/documents/2012/january/competes_010511_0.pdf.

[6] See "Air Force Cyber Vision 2025" by AF/ST.

[7] Network Resilience: A computing infrastructure that provides continuous business operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged), rapid recovery if failure does occur, and the ability to scale to meet rapid or unpredictable demands. (CNSS Instruction 4009).

of mounting commercial pressures at home and abroad, complicated regulatory and contested/congested electromagnetic environments during training and conflict.

3. Balancing the explosion in end-user mobile devices and capabilities with cybersecurity.

4. Addressing Information Security pertaining to data aggregation as the DoD moves to best usages of the cloud.

5. Converging redundant base-level architectures to support different service components, Joint Tenants, and the Intelligence Community (IC).

6. Supporting research toward software-defined networks as contributors to Air Force core missions.

7. Competing successfully to recruit, educate and retain excellent Cyber-Airmen for government service in a highly-dynamic and competitive sector of the U.S. economy.

8. Remaining committed to warfighting systems integration investments in the face of fiscal reductions: integration is the key to a robust, cost-effective military cyberspace domain; investments will need to be made in every modernizing system in order to reap benefits in the coming decade.

Although these challenges are significant, the Information Dominance Vision and Strategy provide consistent, coordinated direction to meet and overcome each.

DIRECTIVE GUIDANCE – INFORMATION DOMINANCE VISION

The Air Force fully exploits the man-made domain of cyberspace to execute, enhance and support Air Force core missions. [8] This vision provides an aim point for coordinated action by many organizations in the Air Force working together to maintain information dominance. [9] The Air Force has defined three prioritized tenets to help guide efforts toward achieving the vision:

1. **Increase effectiveness of Air Force core missions**: The first consideration is contributing to achievement of Air Force core missions - why the Air Force exists as an instrument of national power.

2. **Increase cybersecurity of Air Force information and systems**: The second consideration will then be ensuring Air Force information is secure and the vulnerabilities of systems hosting that information are minimized.

3. **Realize efficiencies through innovative IT solutions**: The third consideration is to resource technology wisely, ensure minimal to no capability gaps or overlaps, shorten our kill chains, rapidly acquire capability, and make better, faster decisions. Innovation is what Airmen do best and cyberspace is rife with opportunities for innovation across mission areas.

Applying theses tenets requires informed judgment by Cyber-Airmen[10] and the support of the Science and Technology, Engineering, and Acquisition communities. The tenets help focus and steer Air Force actions and decision-making about information. Striving to achieve this vision propels us to fully exploit cyberspace.

This information dominance strategy is aligned to the *America's Air Force: A Call to the Future* (Air Force Strategy) and the DoD CIO strategy for information resource management. This strategy is also aligned with the Air Force's Strategic Master Plan (SMP), currently in draft, which will become the authoritative guidance for the Core Function Support Plans (CFSPs).

The four strategic goals[11] outlined below are each supported by a set of specific, measurable, achievable, realistic and time-bound (SMART) objectives[12] designed to meet the goals and overcome the challenges foreseen over the next decade.

[8] Air Force Information Dominance Vision, 2013.

[9] Information Dominance: The operational advantage gained from the ability to collect, control, exploit, and defend information to optimize decision making and maximize warfighting effects." (Air Force Information Dominance Vision).

[10] Cyber-Airmen are specifically trained by the Air Force to directly execute, enhance, and support Air Force core missions in and through cyberspace with a common, air-minded set of cyber-skills. (Air Force Information Dominance Vision).

[11] Goal: An expression of the desired future state of the Air Force in a particular area or theme. Goals define and prioritize broad direction, and are inherently long-term in nature. (Air Force Strategic Master Plan).

[12] Objective: A major milestone or action required to achieve a goal. It produces a tangible result. (Air Force Strategic Master Plan).

STRATEGIC GOALS

To realize the Air Force Information Dominance Vision, the Air Force will execute a set of coherent actions that focus limited resources on achieving the goals and objectives described below. The four goals work in concert with one another. A complete breakdown of goals and supporting objectives are included in Tables 1-4.

Goal 1: Provide Airmen trusted information where they need it so they can be most effective.

Airmen at all levels in the Air Force use timely and accurate information to make informed decisions. The Air Force will achieve greater collaborative efficiency across the DoD and with external mission partners by bringing Air Force IT architectures, systems and processes into compliance with the Joint Information Environment. We will compress the information flow within the kill chain toward the speed of light and apply common data standards in all mission areas. Air Force core missions benefit from this through greater operational and technical resilience, improved interoperability and effectiveness, faster capability delivery, prioritized secure capabilities, and reduced costs.

Goal 2: Organize, train and educate Cyber-Airmen to be experts in cyberspace and the Air Force core missions to which they contribute.

The Air Force will continue its long-standing tradition of being innovative, especially in leveraging cyberspace. We will improve our policies and training/education programs to foster a workforce of highly qualified Cyber-Airmen who execute, enhance and support Air Force core missions. Cyber-Airmen will be experts not only in cyberspace, but in the core missions to which they contribute.

Goal 3: Strengthen mission assurance through freedom of maneuver in and through cyberspace.

Air Force cyberspace capabilities will be built and operated as part of a joint global enterprise that more readily identifies and responds to cyberspace degradation and attack. Air Force cyberspace operations will provide required capabilities to combatant commanders and will continue to improve mission assurance[13] for the Air Force core missions. The Air Force will integrate cybersecurity throughout weapon system development in all mission areas and will focus efforts on keeping information secure. As a man-made domain, cyberspace is fertile ground for game-changing innovation. Innovative ideas of our Airmen will be rapidly identified, vetted, funded, and implemented across the Air Force to maximize potential and

[13] Mission Assurance definition: process to protect or ensure the continued function and resilience of capabilities and assets—including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains—critical to the execution of DoD mission-essential functions in any operating environment or condition. (DODD 3020.40, *DoD Policy and Responsibilities for Critical Infrastructure*)

meet future Air Force needs. Innovations will be sought to shorten the kill chain, increase the speed of decision-making and realize cost savings in order to enhance Air Force core missions.

Goal 4: Optimize the planning, programming and execution of cyberspace investments.

Investments and spending on cyberspace capabilities across the core functions will be fully transparent and aligned with this strategy and subsequent roadmaps. The Air Force will use a flexible and dynamic process of Capital Planning and Investment Control (CPIC)[14] for cyberspace technology to ensure its competitive advantages are realized and to maximize investments expected to enhance Air Force core missions. Improved alignment of spending will provide additional resources for modernization and further innovation.

Supporting Objectives

GOALS	***Supporting Objectives***
1. Provide Airmen trusted information where they need it so they can be most effective	1.1: Develop the full AF Enterprise Architecture by 4Q FY16
	1.2: Deploy an Authentication Infrastructure to dynamically control authorized user access to information by 4Q FY19
	1.3: Divest of those organic services DISA provides as an Enterprise Service NLT 2 FYs after the service is available from DISA
	1.4: Increase interoperability by standardizing all Air Force connectivity to the DoDIN by 4Q FY22
	1.5: Close all Air Force-only data centers by 4Q FY17
	1.6: Move to a resilient JIE SSA[15] by aligning all AF bases behind a JRSS[16] by 4Q FY19
	1.7: Develop a roadmap for implementing DoDI 8320.02 data standards by 4Q FY15
	1.8: Reduce cost (man-hours and dollars) of Records Management by 50% by 4Q FY17
	1.9: Modernize AF Spectrum Management process IAW Joint Electromagnetic Spectrum Operations CONOPS, including adopting the DoD Spectrum Management System by FY17
	1.10: Develop a roadmap to enable information sharing or interoperability and collaborative agreements with allies and coalition partners for

[14] CPIC is an IT portfolio-driven management process for ongoing identification, selection, control and evaluation of investments. This process attempts to link budget activities and agency strategic priorities with achieving specific IT program modernization outcomes. (DOD/DCMO "Guidance for Defense Business Systems Funds Certification and Defense Business System Integrated Program/Budget Review").

[15] Standard Security Architecture.

[16] Joint Regional Security Stack.

	implementation in FY19
	1.11: Upgrade entire SL3CS fleet to Everything-Over-IP architecture by 4Q FY19
	1.12: Analyze and upgrade or eliminate Mission Support Systems by at least 50% by FY20
	1.13: Ensure continuity of service and improve AFCOLs[17] reporting time during transition to AFIMSC[18] by 1Q FY16
2: Organize, train and educate Cyber-Airmen to be experts in cyberspace and the Air Force core missions to which they contribute	2.1: Lead DoD by developing a cyber-ASVAB test to assess cyberspace aptitude of potential recruits by 4Q FY17
	2.2: Attract and retain recruits with prior cyber-skills, experience and certification with incentive programs by 4Q FY18
	2.3: Ensure every Cyber-Airmen position in the Air Force has formal IQT associated with it by 4Q FY 19
	2.4: Shorten the requirement-to-delivery cycle for cyber-training by 75% NLT FY17
	2.5: Produce Cyber-Squadron of the Future CONOPs to improve mission assurance to the weapon system(s) at the wing-level in each MAJCOM by 3Q FY15
	2.6: Require programs to field equipment first to the school house to ensure Cyber-Airmen are trained on the equipment they will operate and maintain by 4Q FY17
	2.7: Evolve Air Force Network Operations Squadrons to be compliant with JIE EOC standards by 4Q FY17
	2.8: Develop and implement a future plan for the SAF/CIO A6 functional authority Administration and Postal missions by 4Q FY17
3: Strengthen mission assurance through freedom of maneuver in and through cyberspace	3.1: Further develop and implement education and training programs to all Airmen to raise awareness of cybersecurity threats applicable to their core mission by 4Q FY17
	3.2: Enable and implement "Cyber Secure" weapons systems design, engineering, and testing with experienced cyber professionals by 4Q FY17
	3.3: Amend the cybersecurity certification process to include a risk management framework process NLT 4Q FY16
	3.4: Establish processes and develop capabilities to protect and defend Air Force information networks and associated systems as a single environment

[17] Air Force Common Output Level Standards.

[18] Air Force Installation & Mission Support Command.

	by 4Q FY18
	3.5: Develop and implement an operational cyberspace C2 construct NLT 2Q FY16
	3.6: Improve dissemination and develop penetration metrics for DAMO[19] and DIB[20] reports and analytics to facilitate corrective actions for Air Force missions by 1Q FY16
	3.7: Modernize Cryptography in Air Force Systems by 4Q FY19
	3.8: Designate a Cyberspace Innovation Center to identify, vet, fund, and implement information and cyberspace innovations to increase the Air Force's competitive advantages in its core missions. IOC by 4Q FY16
4: Optimize the planning, programming and execution of cyberspace investments	4.1: Transform information and information systems policy by creating a 17-series and separate 37-series of publications by Q4 FY16
	4.2: Establish a Capital Planning and Investment Control Process for implementation in WMA, DIMA, IEMA NLT 2Q FY15
	4.3: Improve effectiveness of the ITGEG/B[21] and integration with associated governance bodies across the mission areas NLT 2Q FY15
	4.4: Enhance the usefulness and standardization of IT Portfolio Management Tools NLT 1Q FY15
	4.5: Improve cybersecurity implementation and reduce procurement hurdles through effective development of Risk Management Framework guidance and Authorizing Official guidance NLT 2Q FY15
	4.6: Transform IT financial management to implement "End-to-End" Plan-Spend-Performance decision making NLT 4Q FY16
	4.7: Increase agility in responding to the technological operational requirements by ensuring key systems are designed, engineered, acquired, and sustained smartly, efficiently and streamline the IT acquisition process. NLT 1Q FY16
	4.8: Release a revised Information Dominance Strategy to inform the Air Force Corporate Process and the AF Strategic Master Plan NLT 3Q of each odd-numbered FY

[19] Damage Assessment Management Office.
[20] Defense Industrial Base.
[21] Information Technology Governance Executive Group/Board.

INITIATIVES

The initiatives highlighted in this section move the Air Force toward achieving its strategic goals and objectives. They are projects or a closely linked set of projects that support our goals.

Joint Information Environment (JIE) (Supports Goals 1 and 3)

The Air Force's information environment evolved and converged as individual mission needs dictated, rather than being designed. The maturation of Joint employment concepts over the past twenty years of conflict has driven an awareness of the advantage of consolidation. Likewise, the need for increased security and situational awareness of the environment as a whole led the DoD to drive towards a JIE[22] that standardizes across the DoD and collapses security boundaries. Warfighting, intelligence, and business or functional systems critical to operations are included in the JIE, as well as common services, such as email and other administrative and collaborative tools, storage and backup.

JIE is operated and managed through a Unified Command Plan using enforceable standards, specifications, and common tactics, techniques, and procedures (TTPs).[23] It will facilitate the exchange of information and intelligence across all DoD components, within a secure, robust and standardized architecture that is better able—through incorporation of standards and practices—to adapt to and incorporate emerging technologies, such as mobile wireless devices and applications. The Air Force will continue to aggressively pursue every opportunity to bring Air Force Information Environment architectures, systems, and processes in compliance with JIE.

Data Center Consolidation

A key advantage of the JIE is the physical consolidation/reduction of network infrastructure needed for the range of Air Force operations. Despite concerted efforts over the past decade to consolidate the network operations on individual bases under the base Network Control Center, the Air Force still has many data centers, each driving facility, energy, technology refresh, security, personnel and licensing costs. The Air Force will rationalize all applications, migrate relevant applications to JIE Core Data Centers, and establish Installation Processing Nodes and Special Purpose Processing Nodes IAW JIE standards. We will close all Air Force-only data centers by 4Q FY17.

Enterprise Services

Enterprise Services fall into four categories: Enterprise Applications (e.g., email), Identity and

[22] The JIE is a secure joint information environment, comprised of shared information technology (IT) infrastructure, enterprise services, and a single security architecture to achieve full-spectrum superiority, improve mission effectiveness, increase security and realize IT efficiencies, JIE CONOPS, 25 Jan 2013.

[23] 4-Star JCS TANK, 6 Aug 12.

Access Management, Infrastructure, and Mobility. Enterprise Services change over time as new services become popular and legacy services become obsolete or vulnerable to attacks.

The DoD CIO in coordination with the Services is providing and planning candidate Enterprise Services to support customer-facing capabilities, machine-to-machine services, and infrastructure services for the entire department. Providing a consistent set of enterprise services will help ensure that joint warfighters and their mission partners can discover, access, and use information assets to achieve mission success, no matter where the information resides. This will provide Airmen with increased capabilities at lower cost to support core missions. The Air Force will divest of those organic services DISA provides as an Enterprise Service NLT 2 FYs after the service is available from DISA.

Single Security Architecture (SSA)

The SSA is a common cybersecurity architecture linking Global Enterprise Operations Centers and other command and control (C2) nodes that oversee and protect the consolidated data centers and installation processing nodes. Coupled with common operational TTP, the SSA will enable global and regional situational awareness and a common operational picture of the cybersecurity environment and quick and accurate defensive cyberspace operations from the global to the regional levels. The Air Force will Move to a resilient JIE SSA by aligning all AF bases behind a Joint Regional Security Stack by 4Q FY19.

Network Normalization

Network Normalization improves the resiliency of modern infrastructure to support mission operations and cyberspace-defense through common networks and TTPs. By consolidating networks that employ common operational standards, the DoD will enable the sharing of resources and infrastructure among multiple capabilities, devices, and services.

Under JIE, the shared IT infrastructure will look, feel, and operate the same regardless of service provider and usage (i.e. mission specific uses). JIE will provide standardized networks to increase mission effectiveness and improve cybersecurity, performance and the ability to connect to the DoDIN through government owned or leased connections by terrestrial, wireless, and satellite links.

Enterprise Operations Center (EOC)

As Air Force core missions have become more integrated and reliant on cyberspace over the past two decades, the Air Force has consolidated C2 of networks and information systems to reduce vulnerabilities and increase resilience. Going forward, the JIE EOC serves as a single entry point and primary executor for DoDIN operations, as well as Defensive Cyberspace Operations (DCO), in designated areas of support. End-state services provided by an EOC will include support to CDCs and assuming operational missions from other EOCs in a failover capacity. Eventually, EOCs will provide computer network defense capabilities to the entire DoD enterprise entities regardless of service affiliation. This will increase security, operational flexibility, and responsiveness. Air Force Cyberspace Component (AFCYBER) units will be functionally integrated with JIE EOCs, as defined by USCYBERCOM C2 constructs. The Air Force will evolve its Network Operations Squadrons to be compliant with JIE EOC standards by 4Q FY18.

Future Air Force Bases (Supports Goals 1, 2, and 3)

While the Air Force continues to integrate our execution capabilities across mission areas and components, we also defend the enterprise "commons" upon which those capabilities we depend to exchange information—the Air Force portion of the cyberspace domain. Architecturally, even as we transition toward the JIE, we will continue to employ a defense-in-depth approach (which informs and complements the security structure in JIE) that involves:

1. Improving situational awareness and cybersecurity by enforcing configuration standards to the device level[24] to facilitate automated reporting, centralized control, and effective vulnerability identification and remediation

2. Collapsing public access points to create a smaller and better integrated "perimeter" that is patrolled by automated sensors and highly trained Cyber-Airmen

3. Deploying TTPs to facilitate insider threat detection and prevention

4. Developing, in cooperation with our sister services and USCYBERCOM, cyberspace mission forces with specific expertise in:

    a. Protecting information systems (though identification and remediation of vulnerabilities, reinforced by targeted training)

    b. Robust cyberspace defenses—particularly of key "cyberspace-terrain" or other high-interest info systems (through specialized engineering)

    c. Intercepting and eliminating malicious activity ("Hunt" teams)

    d. Defending DoDIN mission systems. These crews operate designated weapon systems that provide cyberspace security and control, event analysis, and perimeter defense for the Air Force-provisioned portion of the DoD enterprise

The Air Force will continue to organize, train, and equip to provide for the defense of the Air Force's cyberspace "commons" from Cyberspace Squadrons at our bases, including investment in appropriate tools and training for Cyber-Airmen, architectures that simplify situational awareness and C2, and initiatives that facilitate rapid acquisition of defensive capabilities in

[24] See 24 Air Force's Base Area Network Functional Specification

response to evolving threats.

Base-Level Infrastructure

The virtualization of mission and functional systems in a cloud computing environment offers significant opportunities for savings in base-level infrastructure beyond that achieved in data center consolidation. The Air Force spends close to a billion dollars per year on "wired" base-level IT technology refresh and modifications/extensions of base-level IT infrastructure. The fiber optic networks within and between buildings that support computers, phones, and peripheral/supporting devices are a major cost driver in military construction (MILCON) and in utility costs (power and cooling).

In addition, the proliferation of commercial off-the-shelf (COTS) hardware supporting every mission area at the base level has resulted in many thousands of devices being fielded across every Air Force base without the proper configurations that allow centralized cyberspace operators and defenders to see and protect them. This condition hampers cyberspace domain situational awareness and drives base-level and enterprise manpower requirements by hindering centralized configuration management actions like software upgrades and vulnerability identification and remediation. Virtualization of networks and systems enables two complementary initiatives to address both the cost and the cyberspace defense problems from massive, complex base-level infrastructures:

1. Transition of most users and applications from wired, fixed computer resources to mobile devices capable of supporting personal, official/administrative, and FOUO/unclassified mission applications via voice, video, or data on a single secure platform. "A smartphone in the hands of every Airman" is a powerfully transformative direction, allowing our young "digital natives"[25] to proactively leverage commercial applications and ubiquitous information to solve mission problems.

2. Consequent reduction of base level "wired" infrastructure, focusing resources on implementing and sustaining robust, physically diverse connectivity almost exclusively in support of critical mission assets—a reduction of 60-80% in physical plant. This remaining physical infrastructure will be configured and sensored to maximize cyberspace domain situational awareness and defensibility, enabling cyberspace operators to rapidly identify, characterize, and respond appropriately to any event impacting mission execution, whether natural, accidental, or malicious. Having only mission-critical functions tied to wired infrastructures facilitates the rapid adoption of emerging applications and technologies, and ensures robust backup and continuity of operations capabilities.

[25] Prensky, Marc (2001). "Digital Natives, Digital Immigrants". On the Horizon 9 (5): 1–6.

Combat Communications (Extending Services to the Tactical Edge)

The Air Force will ensure its deployable communications capabilities are sized properly and able to support the following Air Force units and mission areas: Contingency Response Forces (CRF), Theater Air Control System (TACS), deployable Airfield Operations, Air Expeditionary Wing (AEW), Combined/Joint Force Air Component Commander (C/JFACC) and Special Operations units. The primary means of supporting these capabilities is by providing operational commanders the cyberspace tools necessary to C2 their assigned forces. Combat communications systems will be adapted to support the future JIE tactical environment and support operations in disconnected, intermittent, and low bandwidth conditions.

Installation and Mission Support Center (Supports Goals 1, 3 and 4)

The Air Force will consolidate common installation and expeditionary combat support capabilities into a single Air Force Installation and Mission Support Center (AFIMSC). This center will more effectively and efficiently manage common installation resources in today's budget constrained environment. Traditional communication and information tasks across every installation will be standardized and centrally executed within AFIMSC. For example, AFIMSC will support bases' long haul communications contracting, IT asset management, engineering and installation (E&I) plans, and publications management. The resource savings from this consolidation will allow MAJCOMs and mission commanders to refocus on their respective core missions and rely on AFIMSC for those common installation resources. The lead command for cyberspace operations will be freed to concentrate its efforts on exploiting the cyberspace domain to execute, enhance and support the Air Force core missions.

Aerial Layer Network (ALN) (Supports Goal 1)

Airborne networking is an enabler of Air Force and Joint missions, and is increasingly important for future forces that will rely on effective communications for mission success. Accordingly, the Air Force will modernize data link and airborne networking capabilities and, in some cases, recapitalize on aging airborne networking infrastructures. There are several capability gaps—across all Air Force core missions—that result from current and projected deficiencies in tactical data links and airborne networking.

The Joint Aerial Layer Network (JALN) is a system of systems consisting of hardware and software to increase communications between different platforms in tactical environments to enable decision superiority by connecting the right people with the right information at the right time. The JALN will provide both information transport and information transformation capabilities to improve the resiliency of information exchanges and extend the connectivity and ranges for Airmen in the tactical environment and reachback to the DoDIN. By providing robust and resilient connectivity, the JALN will improve the conduct and integration of Air Force core missions.

Senior Leader Communications (Supports Goals 1)

The Air Force actively participates in oversight, integration, and advocacy activities for National Leader Command, Control, and Communication Systems (NLC3S) encompassing three mission areas: presidential and senior leader communications; nuclear command, control, and communications (NC3); and continuity of operations /continuity (COOP). These mission areas are of such importance to the nation that they require the involvement and coordination of many departments and agencies.

Spectrum (Supports Goal 1)

Air Force core missions depend on access to portions of the electromagnetic spectrum. The growth in the complexity of modern military systems and the demand for more and timely information at every echelon is driving an increase in need for improved spectrum management. The electromagnetic environment will be increasingly congested and contested wherever military operations occur. Adversaries are aggressively fielding electronic attack and cyberspace technologies that significantly erode the Air Force's ability to access and use spectrum to conduct military operations.

To ensure adequate access to the congested and contested electromagnetic environment of the future, the Air Force will acquire more efficient, flexible, and adaptable information systems while developing more agile and opportunistic spectrum operations to ensure our forces can complete their missions. To succeed, the Air Force will be able to meet the air component commander's requirements and trust that systems will be interoperable with each other and be able to adapt to a dynamic environment. The Joint Electromagnetic Spectrum Operations (JEMSO) CONOPS, once published, will define the Air Force approach for managing spectrum in future conflicts.

CONTINUOUS EFFORTS

Continuous efforts are ongoing processes and programs

Policy

Policy is a continuous journey that supports all Airmen and their missions. This is especially true in the dynamic environment of cyberspace. To keep policy timely and relevant, SAF/CIO A6 changed its approach and will continue to increase the agility of its policy approach. Once an AFI or AFMAN is published, we will begin writing the next interim change. This requires all stakeholders, from technicians to headquarters subject matter experts to be actively involved in providing feedback. If something is not right or reality has changed, the policy will more rapidly reflect this through interim changes every four to six months: this will provide the Cyber-Airmen in the field the guidance needed to succeed. When it comes time to reissue policy after three to four years, most updates will have already been accomplished through the previous interim changes.

Policy will reflect the Information Dominance tenets in this strategy and be used to drive necessary change. For example, the transition to JIE, cloud computing, and Defense Enterprise E-mail will be partially enabled through the tasks as well as the roles and responsibilities directed in policy. Policy will direct how the Air Force will conduct cyberspace portfolio management, architecture, and governance.

To facilitate this, the Air Force will transform the current outdated SAF/CIO A6 policy framework. Cyberspace Operations, IT Services, Information Assurance/Cybersecurity, and Architecture can no longer be treated as stovepipe policy issues if the Air Force is to maintain its cyberspace operational advantage. We will treat policy as a single portfolio that drives unity of effort. All cyberspace policy currently residing in 10-17 and 33 series policy will be consolidated in a new 17 series, matching the Cyberspace Operations career field AFSC. Those items still falling under SAF/CIO A6 but determined to be outside of cyberspace will be consolidated under the 37 series of policy.

Enterprise Architecture

The Air Force Enterprise Architecture (AFEA) is a strategic information resource that documents the capabilities of the Air Force in terms of its people, processes, and technology and relates those capabilities to the Air Force core missions and strategic vision. The Air Force requires architectures to support decision-making about IT investments and to increase cybersecurity and core mission effectiveness.

The enterprise architecture contains information on the current "as-is" state and a future "to-be" state. The as-is state reflects decisions already made and will provide the basis for future decisions addressing how the Air Force is organized, how it performs its mission, the information exchanges, and the systems and technologies it uses.

The AFEA is a group of Air Force architectures that partitions the Air Force Enterprise into a set of smaller-scope architectures that are developed and managed by separate AF organizations. The intent is to leverage the subject matter expertise throughout the Air Force and enable the development of architectures that directly support and are responsive to decision makers across mission areas. All subordinate architectures will be consistent with the AFEA to support these requirements:

1. Facilitate mission area management, including IT portfolio management.

2. Deliver guidance and context for new architectures.

3. Provide AFEA information to satisfy CIO concerns; e.g., cybersecurity.

4. Enable statutorily-required compliance assessments; e.g., interoperability.

A key component of the enterprise architecture is the technical architecture: the Target Baseline/Implementation Baseline/Operational Baseline (TB/IB/OB) construct. This construct is an enable, specifying the technical direction provided in the Information Dominance Strategy and Mission Area Roadmaps and is critical to manage costs, increase agility, and improve cybersecurity. Each baseline is described below:

1. The Target Baseline (TB) specifies the standards, protocols, and guidance for the future state of the Air Force IT infrastructure.

2. The Implementation Baseline (IB) is the baseline of “in-pipeline”/planned products and their TB-informed/allowed configurations that implement the architecture, standards, and protocols specified in the TB.

3. The Operational Baseline (OB) is the set of IB components appropriately configured and deployed across the Air Force’s IT infrastructure to provide the basis for required warfighter capabilities and performance.

Cybersecurity

Cybersecurity is a critical enabler to the proper execution of Air Force core missions. The persistent and evolving cyberspace threat necessitates a broad risk management approach that encompasses people, culture, and operational processes to improve mission assurance. The Air Force is integrating cybersecurity throughout weapons systems development and program management, focusing efforts to secure information for core missions. To that end, the Air Force will focus on extending its cybersecurity approach along four key lines of effort.

1. Educate and inform all Airmen and industry partners on how malicious software (malware) can infest critical weapons systems platforms. Prevention and education is crucial to achieve lasting success and change in Air Force culture and how we address cybersecurity. This line of effort will focus on ensuring all Airmen not only get the right training, but also the supportive intelligence information to make the right decisions.

2. Enable and implement "Cyber Secure" weapons systems design, engineering, and testing with experienced cyber professionals. Update acquisition processes to ensure early engagement and effective system security engineering from the earliest stages of development will "bake in" cybersecurity. A critical enabler for this effort is ensuring experienced Cyber-Airmen are integrated in key acquisition assignments. Overhauling the certification process and transitioning to the risk management framework will also play a key role in institutionalizing an effective long term risk management process.

3. Third, focus cybersecurity operations for weapon systems and Program Management Offices (PMOs). This will be done by operationalizing cybersecurity from Air Force

Space Command (AFSPC)/24th Air Force (24 AF) to mission systems and weapons systems owners beyond the Air Force Network (AFNET). To do this, an effective process will be established where Air Force Material Command (AFMC) and the acquisition community work with operational commanders to ensure current and future mission systems, weapons systems, functional systems, and maintenance systems will incorporate cybersecurity basics.

4. Finally, establish accountability and ownership of cybersecurity from the cubicle to the flightline. Ensuring effective cybersecurity is everyone's job - the ultimate goal is to ensure our culture changes to accept and implement that concept.

Force Development

A key to operational success is a trained, skilled and ready force. The Air Force will recruit individuals with the required skillsets of academics, experience, and aptitude to provide the foundations for success as Cyber-Airmen. These foundational skillsets will be bolstered through continual education (schoolhouse and professional military education) and employment within units that focus on technical and Air Force core mission competencies driving integration of cyberspace capabilities. We will expand our cyberspace skillsets to include knowledge of commercial, public, and military networks employed by partner nations and adversaries to successfully accomplish air, space, and cyberspace operations including: integrated air defense systems, command and control, supervisory control and data acquisition, space, and airborne networks.

We will also continue to sustain and resource those subsets of our cyberspace forces that we rely on to work in concert with cyberspace component or joint command and control structures to integrate cyberspace effects across the tactical, operational, and strategic levels of war.

The Air Force will be prepared to conduct our core missions in a highly contested cyberspace environment, and in anticipation of that reality, will continue to mature operations crew certification, processes, and TTPs. The Air Force will deliberately cultivate Cyber-Airmen able to dynamically design, build, engineer, and configure within the information environment, defend friendly capabilities and resource from attack through cyberspace, and plan and execute cyberspace operations integrating air-minded expertise to achieve joint/combined forces commander objectives.

The demographics of the cyberspace workforce will change in the coming decade. Elements of today's cyberspace activities—particularly enterprise information services like application hosting and sustainment, system administration and help desk functions—will increasingly align with industry. As our architecture modernizes, the Air Force will transition in favor of increased emphasis on battlefield maneuver (e.g., extension into combat theaters, damage mitigation and vulnerability/attack remediation through tactical and operational engineering, etc.), dynamic configuration/sustainment, defensive, and offensive capability development.

However, to grow and sustain an air-minded force, prevent stagnation and provide leadership opportunities, our Cyber-Airmen will have opportunities to cross-flow between organizations and functions operating at the tactical, operational and strategic levels. Going forward all Cyber-Airmen will be developed into experts not only in cyberspace, but in the core missions to which they contribute.

Governance

The primary governance forum for Air Force Information Dominance issues will be the Information Technology Governance Executive Board (ITGEB). A strengthened enterprise cyberspace governance structure will be in place across mission areas to align accomplishment of milestones and reapportion resources as required to meet priorities. This governance will be connected to and aligned with the overarching DoD and Air Force governance structures.

The goals and objectives in this strategy will be formally linked and strategic items reviewed and decided upon by the ITGEB. Functional representatives will be included in the process to evaluate and foster success across all mission threads and core functions. All subordinate governance structures will deliver relevant input into the ITGEB.

The ITGEB structure provides leadership and guidance for the strategic planning process, as well as oversight of, and accountability for, implementation activities. It is composed of senior Air Force advisory members who guide the actions necessary to achieve the Information Dominance goals and objectives. The governance is defined by AFPDs 33-4 and 33-5, both under revision.

Investment

To help the Air Force optimize the effectiveness of investments in cyberspace, SAF/CIO A6 will perform programmatic reviews and provide investment guidance through a robust Portfolio Management program. SAF/CIO A6 will provide IT/cyberspace investment guidance by strengthening governance processes for IT solutions at the enterprise level to maximize interoperability across core mission areas and provide the means for making decisions and recommendations based upon enterprise strategic planning, integrated architectures, and outcome-based performance measures. It will oversee these investments through the entirety of the Portfolio Management and Capital Planning and Investment Control process. An effective portfolio management and governance process will influence investment decisions within existing corporate processes so that the Air Force efficiently delivers IT solutions effectively meeting core mission needs that are secure and compliant; maximizing mission assurance of Air Force operations in and through the cyberspace domain.

Cyberspace Operations Capability Development

In addition to trained and ready forces, the Air force requires appropriate capabilities to prosecute missions in cyberspace. The Air Force will continue to advance its mission assurance capacity with capabilities that provide timely cyberspace vulnerability and intrusion assessments and advanced DCO. These tools eliminate threats and mitigate damage before they have a negative impact on operations across domains and missions.

The Air Force will continue to develop OCO capabilities that provide the ability to engage key adversary targets, creating effects designed to deny, degrade, disrupt, destroy or deceive these systems or the data residing on them in support of the Combatant Commander. To these ends we will continue to foster relationships with industry, academia, research and development activities, and our national and international partners to invest in the most advanced tools and non-materiel capabilities available for leading edge DCO, OCO, Cyberspace ISR and DoDIN Ops to create the conditions for Air Force core mission execution wherever and whenever needed.

As in other domains, the transition from one military activity to another—such as security to defense, or defense to offense—is often one of context and intent. Cyberspace operations, like operations in the other domains, presents a continuum of activities, unified by centralized C2, established supported/supporting relationships, and validated TTPs. Military networks and systems will come under attack in cyberspace during the earliest phases of hostilities—perhaps as the first indication of hostilities—so the Air Force will continue the seamless merger of DoDIN Ops and DCO. A similar seamless progression naturally arises from DCO into active defensive countermeasures, which are in turn differentiated from offensive actions only by circumstance and intent.

Cyberspace operations rely on the full range of traditional military operations to be conducted under Title 10 (military operations), Title 32 (national guard), Title 50 (war and national defense), authorities and subject to rules of engagement. With their global reach and potentially strategic effects, these activities are a natural extension of Air-minded contributions to joint/combined operations and national defense. In particular, the Air Force's cyberspace capabilities are informed by experience and training, bringing particular focus and emphasis on mission sets such as counter-air, IADS suppression, C2, and counter-space.

PARTNERSHIPS

The Air Force will remain closely partnered with the commercial sector, other government entities, and allies in cyberspace. The Air Force shares important information and cyberspace infrastructures between coalition, government, and industry, and shares the challenges of ensuring information resources are trusted and available. The Air Force will expand the close relationships with interagency partners, including law enforcement and the intelligence community, to identify and pursue threats to the enterprise. We will pursue expanded cyberspace situational and predictive threat awareness through increased information sharing with public, private, and allies. Creating and further developing these relationships will contribute to a robust, secure enterprise architecture, effective threat awareness, and resilient, flexible defense for Air Force core mission success.

SUMMARY

As stated in *America's Air Force: A Call to the Future*, one of the most important responsibilities of a military service is to prepare the force for the challenges of tomorrow, not just the realities of today. This strategy does just that—it outlines the Air Force path for achieving the desired end state in the Information Dominance Vision: ***The Air Force fully exploits the man-made domain of cyberspace to execute, enhance, and support its core missions.*** This strategy strengthens the Air Force's contributions to defense and sovereignty, helping our contributions remain fully realized in and through an increasingly congested and contested cyberspace domain

This strategy was guided by three tenets of Information Dominance, revolving around effectiveness, security, and efficiencies and innovation. Supporting the vision and tenets, four goals were defined that together provide the basis for achieving the strategic end state, not only for today, but into the future despite an austere budgetary and rapidly changing security environment. These goals are soundly based, and fully aligned with the Air Force's five core missions. They integrate and link operations within the cyberspace domain and information environment back to the Air Force vision. This integration occurs across all mission areas and applies to all Airmen.

Of course we will remain prepared to continuously adjust to meet not only emerging threats and demands, but also the changing technological environment around us. We will be innovative, and will understand the warfighters' needs while providing an environment where we maximize use of the global commons to our advantage. The Air Force is steeped in innovation, and we will be bold in how we shape operations in and through cyberspace. Our highly-qualified Cyber-Airmen will enable the application of Global Vigilance – Global Reach – Global Power for America; we will remain unparalleled in our ability to Fly, Fight, and Win in Air, Space, and Cyberspace.

APPENDIX - STRATEGY FRAMEWORK

The Information Dominance strategic framework in Figure 2 illustrates the components.

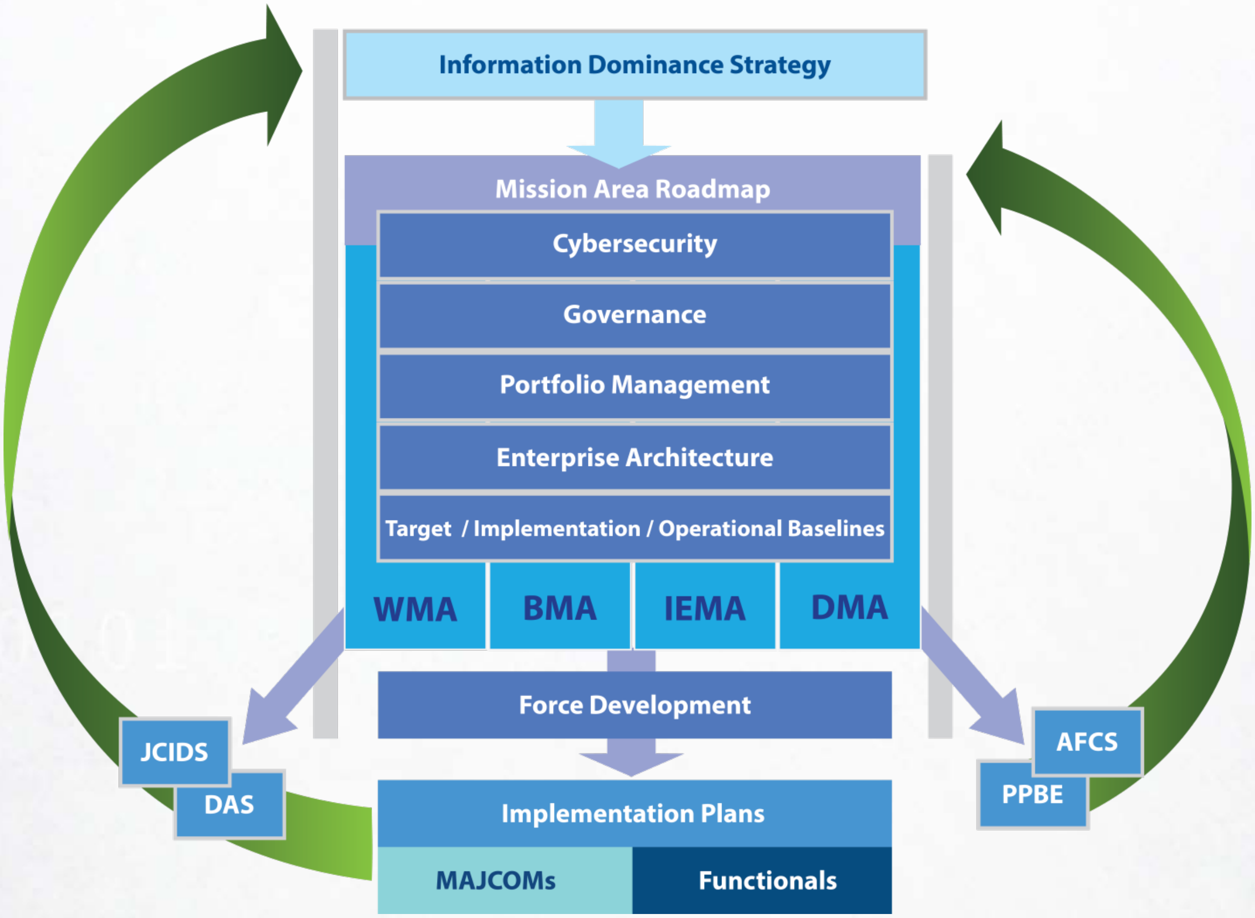


Figure 2. AF Information Dominance Strategy Framework

Strategy

A strategy is a way through a difficulty and an approach to overcoming an obstacle, a response to a challenge. Good strategy discovers critical challenges then designs a coordinated plan of focused actions toward resolution.[26] This strategy is aiming to unify the focus of the Air Force Cyberspace community.

A good strategy works by focusing energy and resources on one, or a very few, pivotal objectives whose accomplishment will lead to a cascade of favorable outcomes. It builds a bridge between the critical challenges at the heart of the strategy and action—between desire and immediate objectives that lie within grasp. Thus, the objectives that a good strategy sets stand a good chance of being accomplished, given existing resources and competencies.

[26] Rumelt, Richard (2011) Good Strategy Bad Strategy: The Difference and Why It Matters. Crown Publishing Group (New York).

Strategy involves focus and, therefore, choice. And choice means setting aside some goals in favor of others. When this hard work is not done, weak strategy is the result.

A good strategy has a basic underlaying structure:

1. **A diagnosis**: an explanation of the nature of the challenge.
2. **A guiding policy**: an overall approach chosen to cope with or overcome obstacles identified in the diagnosis.
3. **Coherent Actions**: steps that are coordinated with one another to support the accomplishment of the guiding policy.

Roadmaps

A roadmap is a plan that matches the short-term and long-term goals with specific solutions to help meet those goals. It is a more detailed description of an initiative or grouping of initiatives supporting a goal(s) and/or objective(s). It is a plan for getting to the desired future state that is sensitive to enterprise architecture, technological, manpower, and budget constraints. Developing a roadmap has three main uses. It helps reach a consensus about a set of requirements and the resources needed to satisfy those requirements; it provides a mechanism to help forecast developments and it provides a framework to help plan and coordinate progress and highlight associated risk.

A roadmap contains details on how capability and services are to be managed, identifying critical paths, shortfall and gaps on the developed solutions.

Mission Area (MA) Roadmaps

There are four DOD-defined MAs: Business Mission Area, Warfighting Mission Area, Enterprise Information Environment Mission Area, and DoD portion of Intelligence Mission Area.[27] A roadmap is required for each of these mission areas to support a coordinated, coherent approach.

Functional / Core Function Lead Roadmaps

These are individual MAJCOM/Functional cyberspace roadmaps that detail how the objectives and elements they are responsible for will be realized.

[27] DODI 8115.02, Information Technology Portfolio Management Implementation.